Optimalisasi Keamanan Jaringan Wireless Menggunakan Firewall Filtering MAC Address

Rachmat Adi Purnama
Teknologi Komputer, Universitas Bina Sarana Informatika
JL. Kamal Raya No. 18, Cengkareng Barat, Cengkareng, Jakarta Barat
rachmat.rap@bsi.ac.id

Abstrak *– Penggunaan layanan jaringan nirkabel 802.11 semakin meningkat, hal ini akan berbanding lurus dengan celah keamanan yang digunakan. Marak terjadinya pencurian dan kebobolan hak akses didalam wireless dikarenakan banyaknya tools yang mudah didapat didalam jaringan internet. Dengan menggunakan keamanan jaringan wireless model WEP/WPA2 yang hanya menerapkan single login untuk melakukan akses kini sudah mudah dibobol, penggunaan keamanan jaringan wireless model Hotspot Login yang melakukan verifikasi terhadap user dan password pun sudah rentan dengan kebobolan hak aksesnya. Untuk meminimalisir terjadinya kebobolan hak akses, penulis menerapkan optimalisasi keamanan jaringan wireless menggunakan metode firewall rule. Metode ini akan melakukan filtering hak akses berdasarkan MAC Address perangkat yang akan terhubung kedalam jaringan. Jadi jika terdapat user yang mencoba melakukan akses kedalam jaringan namun MAC Address dari perangkat tersebut tidak didaftarkan maka perangkat tersebut tidak akan terkoneksi kedalam jaringan internet. Setiap perangkat yang ingin terhubung kedalam jaringan internet harus didaftarkan MAC Addressnya terlebih dahulu.*
Kata Kunci*:Filtering, MAC Address, Firewall Rule, Wireless*

Abstract - *The use of 802.11 wireless network services is increasing, this will be directly proportional to the security gap used. The occurrence of theft and conceding access rights in wireless due to the many tools that are easily available on the internet network. By using wireless network security, the WEP / WPA2 model that only applies a single login to access is now easy to break into, the use of wireless network security Hotspot Login model that verifies users and passwords is already vulnerable to access rights. To minimize the occurrence of conceding access rights, the author applies the optimization of wireless network security using the firewall rule method. This method will filter the access rights based on the MAC Address of the device to be connected to the network. So if there is a user who tries to access the network but the MAC Address of the device is not registered, the device will not be connected to the internet network. Every device that wants to be connected to the internet network must be registered with the MAC Address first.*
Keywords: *Filtering, MAC Address, Firewall Rule, Wireless*

I. PENDAHULUAN

Semakin banyaknya pengguna layanan internet-working maka semakin banyak pula permasalahan dan kendala yang dihadapi didalam dunia teknologi jaringan komputer. 20 tahun terakhir ini, Wireless LAN berbasis 802.11 telah menjadi hal yang umum dilingkungan perkantoran dan dunia kampus [1]. Perkiraan terbaru menunjukan lebih dari 10 miliar perangkat WiFi telah terjual secara total dan lebih dari 4,5 miliar perangkat tersebut digunakan saat ini. Pada jaringan nirkabel, masalah keamanan memerlukan perhatian yang lebih serius, mengingat media transmisi datanya adalah gelombang radio yang bersifat broadcast [2]. Hal ini merupakan salah satu alasan rentannya keamanan didalam jaringan wireless. Kebijakan otentikasi diadopsi untuk mengamankan akses, penyalahgunaan, modifikasi, serta melakukan penolakan terhadap layanan didalam jaringan dan sumber daya lainnya [3]. Banyak pengguna jaringan wireless tidak mengetahui jenis bahaya apa yang sedang menghampiri mereka saat terhubung kedalam Jaringan Wireless Access Point (WAP), misalnya seperti sinyal WLAN yang dapat disusupi oleh hacker [4]. Keamanan wireless WEP (Wired Equivalent Privacy) merupakan standart dari keamanan wireless yang sebelumnya mampu meminimalisir pembatasan hak akses kedalam jaringan wireless. Namun kini keamanan wireless menggunakan WEP sudah mudah dipecahkan dengan berbagai tools yang tersedia didalam jaringan internet.

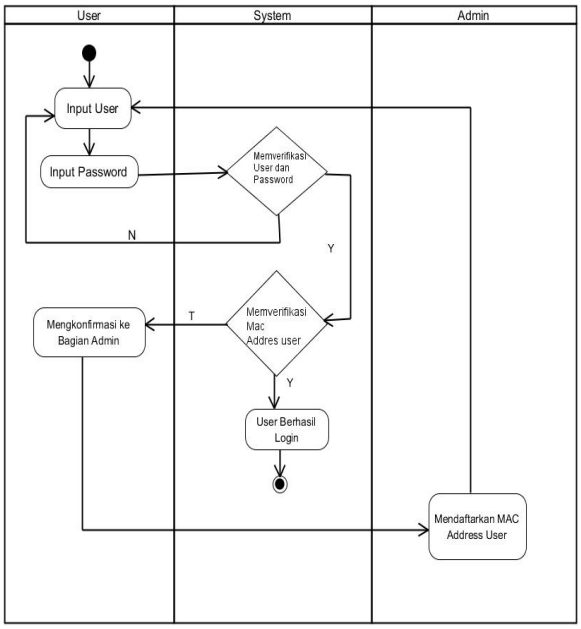
Jaringan nirkabel IEEE 802.11 telah menjadi salah satu jaringan yang paling banyak digunakan [5]. Karena sifat media nirkabel yang terbuka, peretas dan penggangu dapat memanfaatkan internet untuk menemukan celah keamanannya. Kegiatan yang mengancam keamanan jaringan wireless dapat dilakukan dengan cara Warchalking, WarDriving, WarFlying, WarSpamming, atau WarSpying. Untuk memilimalisir pengguna layanan jaringan tanpa melakukan pembayaran dan membatasi akses kedalam jaringan dapat menggunakan sistem keamanan MAC Address Filtering. Metode secu-

rity MAC Address dapat diimplementasikan menggunakan metode Filter Rule. Metode ini dapat bekerja melakukan filtering terhadap perangkat yang mencoba melakukan akses kedalam jaringan komputer.

MAC Address merupakan sebuah identifikasi unik yang terdiri dari berbagai bilangan byte yang ditugaskan untuk sebagian besar adapter jaringan atau Network Interface Card (NIC) [6]. Setiap perangkat jaringan memiliki MAC Address yang berbeda satu dengan lainnya. Maka dengan menerapkan security MAC Address setiap pengguna layanan jaringan yang ingin terhubung kedalam jaringan harus melakukan pendaftaran MAC Addressnya. Hal ini dapat digunakan untuk meminimalisir pengguna layanan jaringan yang seharusnya tidak mendapatkan akses. *Firewall filtering* MAC Address telah dikembangkan untuk memberikan perlindungan terhadap pelayanan jaringan wireless. Penggunaan filtering MAC Address mampu membatasi beberapa komputer yang dapat terhubung kedalam wireless hotspot dengan mempertimbangkan IP Address dan MAC Address yang terdaftar [7]. Diharapkan pengimplementasian keamanan secara ganda mampu meningkatkan keamanan didalam jaringan komputer. Kerena pemakaian frekwensi yang sifatnya lebih terbuka dibanding dengan menggunakan kabel, maka kerentanan keamanan jalur komunikasi akan lebih berbahaya dibandingkan menggunakan kabel. Untuk itu perlu dilakukan penanganan keamanan yang lebih ekstra pada jaringan wireless [8].

2. METODE PENELITIAN

Dalam melakukan penelitian optimalisasi keamanan jaringan wireless menggunakan firewall filtering mac address penulis menggunakan bantuan perangkat mikrotik routerboard 951Ui-2HND yang diimplementasikan menggunakan mode access point 2,4 GHz untuk menghubungkan dengan jaringan lokal dan menggunakan 2 (dua) buah laptop yang akan dijadikan sebagai client untuk melakukan uji konektifas terhadap keamanan jaringan yang digunakan.



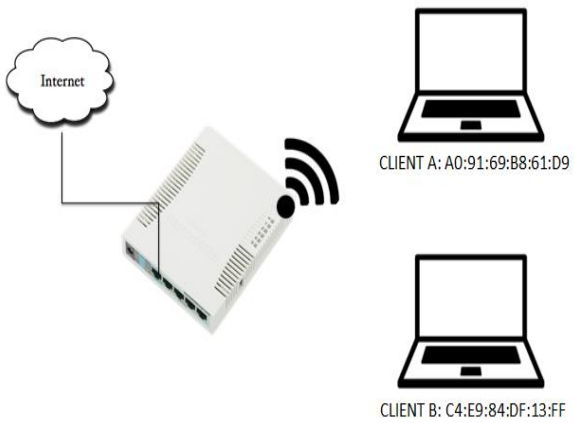
Gambar 1. Activity Diagram

Terlihat pada gambar 1 merupakan alur yang digunakan dalam penelitan optimalisasi keamanan jaringan wireless menggunakan firewall filtering mac address. Client yang akan melakukan akses kedalam jaringan internet harus melewati verifikasi keamanan sebanyak 2 (dua) kali yaitu verifikasi terhadap user dan password menggunakan metode hotspot login, serta verifikasi terhadap MAC Address perangkat menggunakan firewall filtering. Penerapan model keamanan berganda ini bertujuan untuk meminimalisir terjadinya kebocoran terhadap hak akses didalam jaringan wireless. Jika client hanya mengetahui user dan password saja tanpa mendaftarkan MAC address-nya, maka client tersebut tidak dapat melakukan akses kedalam jaringan internet.

3. HASIL DAN PEMBAHASAN

3.1 Skenario Simulasi

Untuk mengimplementasikan optimalisasi keamanan jaringan wireless menggunakan firewall filtering mac address penulis menggunakan skema jaringan yang terlihat pada gambar 2 dengan spesifikasi IP *Address* yang terlihat pada Tabel 1. Dari skema jaringan yang digunakan terlihat pada gambar 2, client A menggunakan MAC Address A0:91:69:B8:61:D9, sedangkan client B menggunakan MAC Address C4:E9:84:DF:13:FF. Client A dan client B nantinya sama-sama akan melakukan verifikasi user dan password pada menu hotspot login dengan menggunakan user dan password yang sama. Untuk melakukan pengujian terhadap firewall filtering, client yang didaftarkan MAC Addressnya hanyalah client A dan client B tidak didaftrakan.



Gambar 2. Skema Jaringan

Tabel 1. Spesifikasi IP Address

Device	Interface	IP Address
Router	Ether1	192.168.137.254
	Ether2	192.168.2.1
Laptop	WLAN	192.168.10.1

Terlihat pada table 1, merupakan spesifikasi IP address ayng digunakan dalam jaringan pengimplementasian jaringan firewall filtering mac, interface ether1 terhubung kedalam jaringan internet dan interface ether2 terhubung dengan network administrator untuk melakukan monitoring didalam jaringan serta interface WLAN digunakan untuk jaringan wireless pada jaringan local.

3.2 Konfigurasi DHCP Server

Routerboard MikroTik memiliki banyak fitur, salah satunya adalah fitur DHCP Server yang banyak digunakan pada jaringan wireless. Pengimplementasian jaringan wireless dipastikan tidaklah luput dari penggunaan DHCP Server. DHCP Server digunakan sebagai fasilitator terhadap client untuk melakukan akses kedalam jaringan komputer. Pengimplementasian DHCP Server digunakan terhadap interface wlan1 pada mikrotik, terlihat pada gambar 3.

```
[admin@MikroTik] > ip dhcp-server pr
Flags: X - disabled, I - invalid
 #   NAME            INTERFACE          RELAY       ADDRESS-POOL          LEASE-TIME ADD-ARP
 0   dhcp1           wlan1                          hs-pool-1             1h
```

Gambar 3. DHCP Server

```
[admin@MikroTik] > ip hotspot user print
Flags: * - default, X - disabled, D - dynamic
 #   SERVER          NAME                ADDRESS     PROFILE                 UPTIME
 0 * ;;; counters and limits for trial users
                     default-trial                                           0s
 1                   admin                           default                 0s
 2                   client                          default                 0s
```

```
[admin@MikroTik] > ip hotspot user profile print
Flags: * - default
 0 * name="default" idle-timeout=none keepalive-timeout=2m status-autorefresh=1m shared-users=20 add-mac-cookie=yes mac-cookie-timeout=3d
     address-list="" transparent-proxy=no
```

Gambar 4. Hotspot User

Terlihat pada gambar 4, merupakan hotspot user yang digunakan untuk mendukung pengimplementasian DHCP Server terhadap jaringan wireless. Terdapat 2 (dua) user yang dapat melakukan akses kedalam jaringan komputer yaitu user admin dan user client. Setiap pengguna layanan jaringan akan diminta melakukan verifikasi pada hotspot login dengan menggunakan user dan password yang telah didaftarkan pada hotspot user. Namun sistem keamanan yang terbatas pada fitur hotspot login dapat menjadi sebuah celah dari kebocoran user dan password terhadap jaringan wireless yang digunakan dikarenakan bersifat broadcast.

3.3 Konfigurasi Firewall Rule

Jika mengacu terhadap gambar 4, setiap pengguna layanan yang ingin melakukan akses kedalam jaringan komputer harus melakukan verifikasi pada hostpot login. Skenario pengujian adalah Client A maupun client B dapat menggunakan user dan password yang sama untuk melakukan login kedalam jaringan komputer. Namun, client B tidak dapat melakukan akses kedalam jaringan internet dikarenakan MAC Address dari perangkat client b tidak didaftarkan kedalam filtering MAC Address didalam jaringan.

```
[admin@MikroTik] > interface wireless registration-table pr
 # INTERFACE                                RADIO-NAME      MAC-ADDRESS       AP SIGNAL-STRENGTH TX-RATE UPTIME
 0 wlan1                                                    A0:91:69:B8:61:D9 no  -29dBm@1Mbps   54Mbps   3m
[admin@MikroTik] > ip arp pr
Flags: X - disabled, I - invalid, H - DHCP, D - dynamic, P - published, C - complete
 #   ADDRESS         MAC-ADDRESS       INTERFACE
 0 DC 192.168.2.2    14:DA:E9:63:AA:5E ether2
 1 DC 192.168.137.1  44:1E:A1:CE:87:95 ether1
 2 DC 192.168.10.254 A0:91:69:B8:61:D9 wlan1
```

Gambar 5. IP ARP

Dijelaskan pada gambar 5, merupakan ARP yang menampilkan data IP Address serta MAC Address client yang sudah melakukan akses kedalam jaringan komputer. Client A mendapatkan alokasi IP Address 192.168.10.254 secara DHCP dengan menggunakan MAC Address A0:91:69:B8:61:D9. Untuk mengimplementasikan pembatasan hak akses menggunakan filtering MAC Address dapat menggunakan metode filter rule dengan mendaftarkan satu per satu MAC Address yang akan diizinkan melakukan akses kedalam jaringan. Hal ini digunakan untuk mengoptimalkan keamanan jaringan wireless dengan menerapkan keamanan berlapis hotspot login dan filtering MAC Address.

//chain=forward action=accept in-interface=wlan1 out-interface=ether1 scr-mac-address= A0:91:69:B8:61:D9 log=no log-prefix=" "

//chain=forward action=drop in-interface=wlan1 out-interface=ether1 log=no log-prefix=" "

Konfigurasi tersebut merupakan pengimplementasian filtering MAC Address dengan mendaftarkan MAC Address client A agar dapat terhubung kedalam jaringan wireless. Saat ini hanya perangkat dari client dengan MAC Address A0:91:69:B8:61:D9 saja yang diberikan hak akses untuk melakukan akses kedalam jaringan internet pada jaringan wlan1. Untuk perangkat yang tidak didaftarkan MAC Addressnya maka perangkat tersebut tidak dapat melakukan konektifitas kedalam jaringan komputer walaupun mengetahui user dan password dari hotspot login.

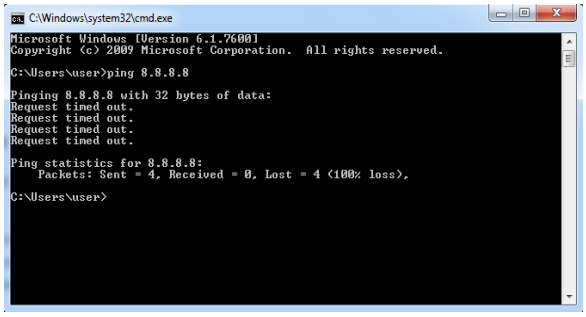
3.4 Uji Konektifitas Drop

Uji konektiftas yang pertama kali dilakukan ialah melakukan percobaan akses kedalam jaringan wireless dari client. Client B mencoba melakukan akses kedalam jaringan dengan menggunakan user dan password yang digunakan pada hotspot login Mikrotik. Ketika verifikasi user dan password diterima pada hostpot login, maka client B akan mendapatkan alokasi IP Address secara otomatis walaupun MAC Addressnya tidak didaftarkan pada filter rule mikrotik. Dengan pengimplementasian Filtering MAC Address, pengguna yang mencoba melakukan akses kedalam jaringan komputer namun MAC Addressnya tidak didaftarkan maka client tersebut tidak akan terhubung kedalam jaringan internet. Hal ini dikarenakan sistem keamanan jaringan wireless telah menggunakan keamanan berlapis dengan menerapkan keamanan verifikasi hotspot login dan filtering MAC Address. Terlihat pada gambar 8 dan gambar 9 merupakan hasil pengujian dari client B yang melakukan percobaan akses terhadap jaringan komputer dan jaringan internet.

Tabel 2. Uji Konektifitas 1

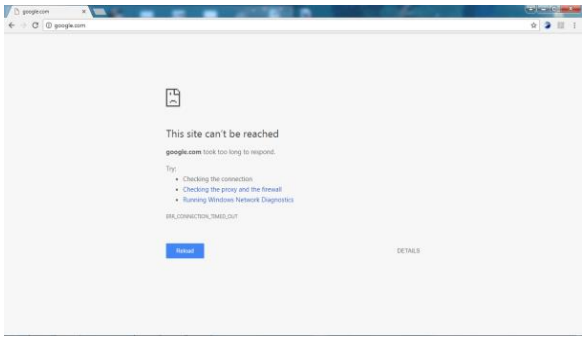
Device	MAC Address	DHCP Client	Internet
Client A	A0:91:69:B8:61:D9	Yes	Yes
Client B	C4:E9:84:DF:13:FF	Yes	No

Table 2 menjelaskan hasil uji konektifitas dari jaringan firewall filtering MAC address, dijelaskan client A mendapatkan alokasi IP Address secara DHCP dan dapat melakukan akses kedalam jaringan internet. Sedangkan client B hanya mendapatkan alokasi IP Address secara DHCP dan tidak mendapatkan akses untuk melakukan konektifitas kedalam jaringan internet.



Gambar 8. Test ICMP

Uji konektifitas pengiriman paket ICMP dari sisi client B tidak dapat berjalan walaupun client tersebut mendapatkan alokasi IP Address, terlihat pada gambar 8. Serta, pengujian akses terhadap HTTP ataupun HTTPS dari sisi client B pun tidak dapat berjalan, terlihat pada gambar 9. Hal ini dikarenakan semua MAC Address yang tidak terdaftarkan diberikan action=drop pada firewall rule.



Gambar 9. Test HTTP

3.5 Uji Konektifitas Accept

Uji konektifitas jaringan skenario 2, peneliti mencoba untuk memberikan hak akses terhadap client B dengan MAC Address C4:E9:84:DF:13:FF agar dapat terkoneksi kedalam jaringan komputer. Jika melihat pada gambar 8 dan gambar 9 MAC Address tersebut mencoba melakukan akses kedalam jaringan namun tidak berhasil.

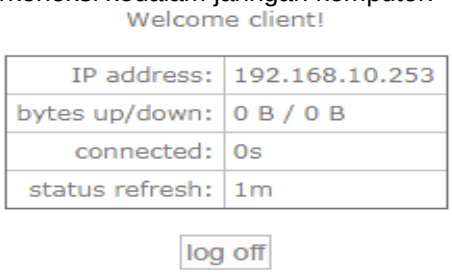
//chain=forward action=accept in-interface=wlan1 out-interface=ether1 scr-mac-address= A0:91:69:B8:61:D9 log=no log-prefix=" "

//chain=forward action=accept in-interface=wlan1 out-interface=ether1 scr-mac-address= C4:E9:84:DF:13:FF log=no log-prefix=" "

//chain=forward action=drop in-interface=wlan1 out-interface=ether1 log=no log-prefix=" "

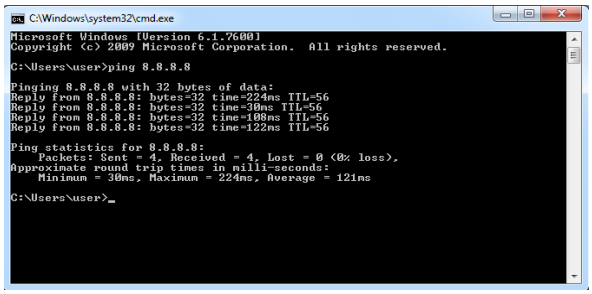
Konfigurasi penambahan database terhadap MAC Address C4:E9:84:DF:13:FF pada

filter rule harus mempertimbangkan tingkatan prioritas dari MikroTik. Dikarenakan jika MAC Address yang baru ditambahkan berada dibawah prioritas dari action=drop maka keseluruhan MAC Address yang baru ditambahkan akan tetap tidak terkoneksi kedalam jaringan komputer.



Gambar 10. Hotspot Login Client MAC Address C4:E9:84:DF:13:FF

Terlihat pada gambar 10 dan gambar 11, client B dengan MAC Address C4:E9:84:DF:13:FF telah didaftarkan MAC Addressnya dan akan mendapatkan alokasi IP Address dan Hak Akses untuk dapat melakukan akses kedalam jaringan internet dikarenakan action yang digunakan telah berubah dari drop menjadi accept. Client B mendapatkan alokasi IP Address 192.168.10.253 dengan menggunakan subnet 255.255.255.0.



Gambar 11. Test ICMP 2

Dijelaskan pada gambar 11 dan table 3, merupakan hasil dari uji konektifitas jaringan yang dilakukan sisi client B yang sebelumnya client B tidak dapat melakukan akses kedalam jaringan, kini client B sudah dapat terkoneksi dan terhubung kedalam jaringan internet.

Tabel 3. Uji Konektifitas 2

Device	MAC Address	DHCP Client	Internet
Client A	A0:91:69:B8:61:D9	Yes	Yes
Client B	C4:E9:84:DF:13:FF	Yes	Yes

4. KESIMPULAN

Pengimplementasian filtering MAC Address mampu mengoptimalkan keamanan jaringan wireless dikarenakan menggunakan keamanan jaringan berlapis selain menggunakan keamanan dengan melakukan verifikasi user dan password terhadap hotspot login, penerapan firewall rule MAC Address dapat digunakan untuk membatasi hak akses berdasarkan MAC Address perangkat. Hal ini sangat berguna dikarenakan ferkuensi yang digunakan pada jaringan wireless bersifat broadcast. Jika terdapat client yang mencoba melakukan percobaan akses kedalam jaringan komputer akan tetapi perangkat dari client tersebut tidak didaftarkan maka perangkat dari client tersebut tidak akan terkoneksi kedalam jaringan internet. Untuk mendapatkan akses kedalam jaringan internet setiap perangkat harus trlebih dahulu didaftarkan MAC Address perangkatnya.

DAFTAR PUSTAKA

[1] F. Wamser, R. Pries, D. Staehle, K. Heck, and P. Tran-Gia, “Traffic characterization of a residential wireless Internet access,” *Telecommun Syst*, vol. 48, no. 1, pp. 5–17, 2011.

[2] D. Yuniarto, “Keamanan Jaringan Wireless LAN menggunakan MAC Address di SMK Informatika Sumedang,” *J. Infoman’s*, vol. 3, no. 1, pp. 47–52, 2019.

[3] N. Ag and G. Shankar, “A Survey on Wireless Security Standards and Future Scope,” *Int. J. Latest Res. Eng. Technol.*, vol. 02, no. 08, pp. 94–99, 2016.

[4] A. Tedyyana, “Rancang Bangun Jaringan Wirelless Di Politeknik Negeri Bengkalis Menggunakan MAC Filtering,” in *SENIATI 2016*, 2016, pp. 31–36.

[5] M. Waliullah, A. B. M. Moniruzzaman, and M. S. Rahman, “An Experimental Study Analysis of Security Attacks at IEEE 802.11 Wireless Local Area Network,” *Int. J. Futur. Gener. Commun. Netw.*, vol. 8, no. 1, pp. 9–18, 2015.

[6] F. Zuli and A. Priambodo, “Analisis Keamanan Jaringan Nirkabel Publik Dengan Radius (Studi Kasus Univeristas Satya Negara Indonesia – Fakultas Teknik,” *J. Ilm. Fak. Tek. LIMIT’S*, vol. 13, no. 1, pp. 8–18, 2017.

[7] R. D. Sari, Supiyandi, A. P. U. Siahaan, M. Muttaqin, and R. B. Ginting, “A Review of IP and MAC Address Filtering in Wireless Network Security,” *IJSRST*, vol. 3, no. 6, pp. 470–473, 2017.

[8] A. Supriyanto, “Analisis Kelemahan Keamanan pada Jaringan Wireless Aji,” *J. Teknol. Inf. Din. Vol.*, vol. XI, no. 1, pp. 38–46, 2006.